WHAT IS CLAIMED IS:

1. A protective device for internal resource protection in a network, comprising:

a firewall between an internal network and an external network, to selectively perform a disconnection function for an access request to the internal network from the external network;

a FTP proxy to perform an authentication function for an access request from the internal network to the external network and to record copies of data transmitted to the external network and log information related to the transmission of data by an authenticated user;

a file system to store data transmitted from the internal network to the external network according to the control of the FTP proxy; and

a database to store log information related to the transmission of data according to the control of the FTP proxy.

2. The device of claim 1, further comprising a proxy monitor configured to display the log information outputted from the FTP proxy.

3. The device of claim 1, wherein a client can connect to a FTP server of the external network through the FTP proxy.

4. The device of claim 1, wherein the log information comprises a file name and absolute path of the file data to be stored in the FTP server, and a file name and absolute path of the file data logged on the FTP proxy.

5. A method for protecting internal resources in a network, comprising:

determining whether an access request for accessing an external network from an internal user of an internal network is permitted or not;

connecting to a server located in the external network if the access request is permitted;

receiving a service command from the internal user;

if the received service command is a command designating a type of data, storing the designated type of data; and

if the received service command is a command requesting data transmission, transmitting data from the internal user and recording the transmission and reception of services.

6. The method of claim 5, wherein the step of determining whether an access request is permitted comprises:

determining whether an ID transmitted from the internal user is a registered ID or not; and

controlling access by determining whether a host that has transmitted the access request is a registered host or not, if the ID of the internal user is a registered ID.

7. The method of claim 6, wherein the access control step comprises:

reading host information corresponding to the registered ID from an internal database using the registered ID;

determining whether the host information read from the database and the host that has transmitted the access request are identical or not;

permitting access to the external network if the two hosts are identical.

8. The method of claim 5, wherein access control is not performed if the ID transmitted from the internal user is "Anonymous".

9. The method of claim 5, wherein the step of transmitting data comprises:

checking an ID of the internal user if the received service command is a command requesting data transmission;

if the user ID is "Anonymous," interrupting the transmission of the received service command to the external network; and

if the user ID is a registered ID other than "Anonymous," transmitting the received service command to the external network and transmitting the data received from the internal user to the external network.

10. The method of claim 5, wherein recording the transmission and reception of services comprises:

receiving file data to be transmitted from the internal user to the external network;

identifying the file data according to its data type to store the file data in the file system; and

recording log information on the transmission of file data in a database.

11. The method of claim 10, wherein the filed data can be identified by the user as a designated data type or can be identified as a default data type.

12. The method of claim 10, wherein the log information is recorded in the database when all data to be transmitted from the internal user to the external network is transmitted.

13. The method of claim 10, wherein the log information comprises a file name and absolute path of the file data to be stored in the FTP server, and a file name and absolute path of the file data logged on the FTP proxy

14. A method for protecting internal resources in a network, comprising:

giving an internal user of a local network in which a firewall is built a proper ID and host information;

performing authentication and access control upon receiving a request for access to an external network from the internal user;

connecting to a server of the external network if an access to the external network is permitted; and

receiving a service command from the internal user, and if the service command is a request for data transmission, transmitting file data transmitted from the internal user to the server and storing copies of the transmitted file data and log information in a database.

15. The method of claim 14, wherein the authentication and access control comprises:

determining whether the ID transmitted from the internal user is a registered ID;

if the ID is registered, reading host information corresponding to the registered ID from the database;

determining whether the host information read from the database and the host who has transmitted the access request are identical; and

permitting access to the external network if the two hosts are identical.

16. The method of claim 14, wherein storing copies of the transmitted file data and log information comprises:

receiving file data to be transmitted from the user to the external network;

identifying the file data according to a data type to thus store the file data in the file system; and

recording log information regarding the transmission of file data in a database.

17. The method of claim 16, wherein the log information comprises a user ID for performing file data transmission, a source IP address of the client being used by the internal user, a destination IP address of the FTP server that receives the file data, a date and time of file data transmission, a file name and absolute path of the file data to be stored in the FTP server, and a file name and absolute path of the file data logged on the FTP proxy.

18. The device of claim 1, wherein the file system stores data according to a type of the data.

19. The device of claim 18, wherein the type of data is at least one of ASCII, EBCDIC, and Image.

20. The device of claim 1, further comprising a client, coupled to the firewall and to the FTP proxy, to request FTP service from the external network if the FTP proxy successfully authenticates the client.

21. The method of claim 10, further comprising outputting the log information in a form recognizable to a system operator.

22. The method of claim 16, further comprising outputting the log information in a form recognizable by a system operator.